UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,730	03/31/2004	Bruce Edward LaVigne	200314975-1	5129

22879 7590 10/24/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
ALMEIDA, DEVIN E	
ART UNIT	**PAPER NUMBER**
2432	

NOTIFICATION DATE	DELIVERY MODE
10/24/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/813,730	LAVIGNE ET AL.	
	Examiner	Art Unit	
	DEVIN ALMEIDA	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 12/27/2007. Claims 1-23 were received for consideration.

Response Arguments

Applicant's arguments with respect to no showing that the provision application 60/466,268 of Regan discloses support for the claimed subject matter have been fully considered but they are not persuasive. The provision application 60/466,268 clearly teaches on page 3 receiving a data packet to be remotely mirrored by an entry device pre-configured with a mirroring destination address to which to mirror the data packet; forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet and a copy to a mirror destination (see page 3 i.e. Mirroring packets as they appear on the wire is very important for troubleshooting encapsulation and protocol level issues. The FlexPath NPA preserves the ingress packet throughout the forwarding process, making incremental packet changes on a separate copy. If a mirroring decision is made at ingress, the NPA sends the original ingress packet to the mirror destination while performing normal forwarding on the other version of the packet. When performing egress mirroring, the NPA performs normal packet handling on the egress packet, encapsulating it for the destination interface. A copy of the forwarded packet (as seen on the wire) is forwarded to the mirror destination); and forwarding the encapsulated packet to an exit device associated with the mirroring destination address (see page 3 i.e. Mirror destinations may be local (egress interface) or remote. Remote destinations are reached via encapsulating the ingress or egress

packet within a service tunnel. At the remote destination, the tunnel encapsulation is removed and the packet is forwarded out a local egress interface).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 7-10, and 14-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Regan (U.S. 2004/0213232) in view of Amara et al (U.S. Patent # 6,839,338). Regan teaches with respect to claim 1, a method for secure remote mirroring of network traffic, the method comprising:

receiving a data packet to be remotely mirrored by an entry device (see Regan abstract i.e. data packets, segments, frames, or other forms of encapsulation may be mirrored off of a core network (e.g., IP, TCP) to one or more mirroring destinations without using a parallel network)) pre-configured with a mirroring destination address to which to mirror the data packet (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent));

forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet and a copy to a mirror destination (see Regan abstract and paragraph 0022-0026); and

forwarding the encapsulated packet to an exit device associated with the mirroring destination address (see paragraph 0023 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent)).

Regan does not teach encrypting a copy the data packet to form an encrypted packet; incrementing an identifier for indicating a position of the data packet within an order of packets received by the entry device for remote mirroring; generating and adding a header to encapsulate the encrypted data packet, wherein the header includes the destination address.

Regan teaches that the mirrored packet are encapsulated and sent via a transport tunnel (see paragraph 0025) but does not go into the way the packets are encapsulated. Amara teaches encrypting a copy the data packet to form an encrypted packet (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet); incrementing an identifier for indicating a position of the data packet within an order of packets received by the entry device for remote mirroring (see Figure 4 element 210 sequence number and column 8 lines 5-24); generating and adding a header to encapsulate the encrypted data packet, wherein the header includes

the destination address (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet and it places the encrypted packet into a new IP packet).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the encapsulation as taught by Amara to encrypt and encapsulate the data packet to further increase the security of the data packet by not allowing other devices to intercept the IP packet and read its data portion (see Amara column 7 lines 30-39). Therefore one would have been motivated to have used the encapsulation as taught by Amara.

With respect to claim 2, wherein the mirroring destination address comprises an Internet protocol (IP) destination address (see Amara column 9 lines 16-40), wherein the header comprises an IP header (see Amara column 8 line 66 – column 9 line 15 i.e. IP packet); and wherein the encapsulated encrypted packet comprises an IP-encapsulated encrypted packet (see Amara column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet and it places the encrypted packet into a new IP packet).

With respect to claim 7, further comprising: receiving the encapsulated encrypted packet by the exit device (see Amara column 8 line 66 – column 9 line 15 i.e. the destination device endpoint); removing the header to de-encapsulate the encrypted packet; and decrypting the encrypted packet to re-generate the data packet (see Amara column 8 line 66 – column 9 line 15 i.e. the destination device endpoint decrypts the

original IP packet and forwards that packet to the destination device); and using said identifier to determine the position of the data packet within the order of packets received by the entry device for mirroring (see Amara Figure 4 element 210 sequence number and column 8 lines 5-24).

With respect to claim 8, wherein the encrypting and decrypting is performed under a public-private key encryption scheme (see Amara column 10 lines 6-60).

With respect to claim 9, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device (see Amara column 10 lines 6-60).

With respect to claim 10, configuring the entry device in a best effort mirroring mode to reduce head-of-line blocking (see Amara abstract and column 8 line 66 – column 9 line 15).

With respect to claim 11, configuring the entry device in a lossless mirroring mode to assure completeness of mirrored traffic (see Amara abstract and column 8 line 66 – column 9 line 15).

With respect to claim 14, a networking device comprising:

a plurality of ports for receiving and transmitting packets therefrom, wherein the packets are transmitted based on original destination address indicated therein (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent));

a secure remote mirroring engine configured to detect packets from a specified mirror source, and to forward the encapsulated encrypted packets to a pre-configured destination by way of at least one of the ports (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent)).

Regan does not teach to use an incrementing identifier to indicating an order of the detected packets, to encrypt the detected packets, to encapsulate the encrypted packets using a header which includes said identifier, and an encryption module configured to be utilized by the remote mirroring engine during encryption of the detected packets.

Regan teaches that the mirrored packet are encapsulated and sent via a transport tunnel (see paragraph 0025) but does not go into the way the packets are encapsulated. Amara teaches to use an incrementing identifier to indicating an order of the detected packets (see Figure 4 element 210 sequence number and column 8 lines 5-24), to encrypt the detected packets (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet), to encapsulate the encrypted packets (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet and it places the encrypted packet into a new IP packet) using a header which includes said identifier (see Figure 4 element 210 sequence number and column 8 lines 5-24), and an encryption module configured to be utilized by the remote mirroring

engine during encryption of the detected packets (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the encapsulation as taught by Amara to encrypt and encapsulate the data packet to further increase the security of the data packet. Therefore one would have been motivated to have used the encapsulation as taught by Amara.

With respect to claim 15, wherein the pre-configured destination address comprises an Internet protocol (IP) destination address (see Amara column 9 lines 16-40).

With respect to claim 16, The networking device of claim 15, wherein the remote mirroring engine encrypts the copies of the detected packets using a public key of a public-private key pair (see Amara column 10 lines 6-60).

With respect to claim 17, a system for secure remote mirroring of network traffic, the system comprising: a mirror entry device including a secure mirroring engine configured to detect packets from a specified mirror source, and to forward the encapsulated encrypted packets to a pre-configured destination by way of at least one of the ports, wherein the pre-configured destination is distinct from original destination indicated in the detected packets, and wherein the detected packets are forwarding in unencrypted form towards an original destination address indicated in the data packet (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets

from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent)); and a mirror exit device including a secure mirroring receiver configured to detect and decapsulate the encapsulated encrypted packets from the mirror entry device and to decrypt the encrypted packets (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent)).

Regan does not teach to use an incrementing identifier to indicating an order of the detected packets, to encrypt the detected packets, to encapsulate the encrypted packets using a header which includes said identifier, and an encryption module configured to be utilized by the remote mirroring engine during encryption of the detected packets.

Regan teaches that the mirrored packet are encapsulated and sent via a transport tunnel (see paragraph 0025) but does not go into the way the packets are encapsulated. Amara teaches to use an incrementing identifier to indicating an order of the detected packets from the specified source (see Figure 4 element 210 sequence number and column 8 lines 5-24), to encrypt copies of the detected packets using an encryption module (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet), encapsulate the encrypted packets (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet and it

places the encrypted packet into a new IP packet) using a header which includes said identifier (see Figure 4 element 210 sequence number and column 8 lines 5-24).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the encapsulation as taught by Amara to encrypt and encapsulate the data packet to further increase the security of the data packet. Therefore one would have been motivated to have used the encapsulation as taught by Amara.

With respect to claim 18, wherein the encrypting and decrypting is performed under a public-private key encryption scheme (see Amara column 10 lines 6-60).

With respect to claim 19, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device (see c Amara olumn 10 lines 6-60).

With respect to claim 20, a system for secure remote mirroring of network traffic, the system comprising a mirror entry device and a pre-configured destination address associated with a mirror exit device; wherein the pre-configured destination is distinct from original destination indicated in the detected packets, wherein the detected packets are forwarding in unencrypted form towards an original destination address indicated in the data packet (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent)).

Regan does not teach including means to encrypt the detected packets using an encryption module and to encapsulate the encrypted packets using a header which includes said identifier; and the mirror exit device including means to decapsulate the encapsulated encrypted packets from the mirror entry device and to re-order and decrypt the encrypted packets.

Regan teaches that the mirrored packet are encapsulated and sent via a transport tunnel (see paragraph 0025) but does not go into the way the packets are encapsulated. Amara teaches including means to encrypt the detected packets using an encryption module (see Amara column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet) and to encapsulate the encrypted packets (see Amara column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet and it places the encrypted packet into a new IP packet) using a header which includes said identifier (see Amara Figure 4 element 210 sequence number and column 8 lines 5-24); and the mirror exit device including means to decapsulate the encapsulated encrypted packets from the mirror entry device and to re-order and decrypt the encrypted packets (see Amara column 8 line 66 – column 9 line 15 i.e. the destination device endpoint decrypts the original IP packet and forwards that packet to the destination device).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the encapsulation as taught by Amara to encrypt and encapsulate the data packet to further

increase the security of the data packet. Therefore one would have been motivated to have used the encapsulation as taught by Amara.

With respect to claim 21, A method for secure remote mirroring of network traffic, the method comprising:

remotely configuring an entry device with an destination address (see Regan abstract i.e. data packets, segments, frames, or other forms of encapsulation may be mirrored off of a core network (e.g., IP, TCP);

receiving a data packet to be mirrored by the entry device (see Regan abstract i.e. data packets, segments, frames, or other forms of encapsulation may be mirrored off of a core network (e.g., IP, TCP);

forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet and forwarding the encapsulated encrypted packet to the exit device (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent)).

Regan does not teach remotely configuring an exit device at the destination address with a decryption key; incrementing an identifier to indicate a position of the data packets within an order of packets mirrored by the entry device; encrypting a copy of the data packet using the encryption key to form an encrypted packet; generating and

adding a header to encapsulate the encrypted data packet, wherein the header includes the mirroring destination address.

Regan teaches that the mirrored packet are encapsulated and sent via a transport tunnel (see paragraph 0025) but does not go into the way the packets are encapsulated. Amara teaches remotely configuring an exit device at the destination address with a decryption key (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet); incrementing an identifier to indicate a position of the data packets within an order of packets mirrored by the entry device (see Figure 4 element 210 sequence number and column 8 lines 5-24); encrypting a copy of the data packet using the encryption key to form an encrypted packet (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet); generating and adding a header to encapsulate the encrypted data packet (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet and it places the encrypted packet into a new IP packet), wherein the header includes the mirroring destination address (see column 9 lines 16-40);

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the encapsulation as taught by Amara to encrypt and encapsulate the data packet to further increase the security of the data packet. Therefore one would have been motivated to have used the encapsulation as taught by Amara.

With respect to claim 22, wherein the remote configuration is performed by way of SNMP (see Amara column 3 line 14 – column 4 line 17 SNMP is included in TCP/IP).

With respect to claim 23, wherein the remote configuration is performed by way of a secure remote protocol (see Amara column 3 line 14 – column 4 line 17).

Claims 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Amara et al (U.S. Patent # 6,839,338) in view of Regan (U.S. 2004/0213232) in further view of Liu (U.S. 2004/0184408).

With respect to claim 3, wherein the mirroring destination address comprises a media access control (MAC) destination address (see Liu paragraph 0023 i.e. MAC destination address), and wherein the header comprises a MAC header (see Liu paragraph 0020-0022 i.e. MAC header), and wherein the encapsulated encrypted packet comprises a MAC-encapsulated encrypted packet (see Liu paragraph 0023 i.e. MAC–in-MAC packet). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have use the MAC address for the packet since it is a commonly used standard. Therefore one would have been motivated to have used MAC address.

Claim 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Regan (U.S. 2004/0213232) in view of Amara et al (U.S. Patent # 6,839,338) in view of Kojima et al (5,280,476). Rega and Amara teaches everything with respect to claim 2 above but does not teach with respect to claim 4 determining a media access control (MAC) address associated with the destination IP address; generating and adding a MAC header to the IP-encapsulated packet to form a MAC data frame, wherein the MAC header includes the MAC address in a destination field; and transmitting the MAC data frame to communicate the IP-encapsulated packet across a layer 2 domain.

Kojima teaches determining a media access control (MAC) address associated with the destination IP address (see Kojima column 5 lines 17-35); generating and adding a MAC header to the IP-encapsulated packet to form a MAC data frame (see Kojima column 5 lines 5-16), wherein the MAC header includes the MAC address in a destination field ; and transmitting the MAC data frame to communicate the IP-encapsulated packet across a layer 2 domain (see Kojima column 5 lines 5-16 i.e. delivers the resulting data to the local area network). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have added a MAC header to the data get to help the data get delivered to its destination across the LAN (see Kojima column 5 lines 17-35). Therefore one would have been motivated to have add a MAC header.

With respect to claim 5, wherein determining the MAC address comprises: determining if a mapping of the destination IP address to the MAC address is stored in an address resolution protocol (ARP) cache (see Kojima column 5 lines 17-35); if so, then retrieving the MAC address from the ARP cache (see Kojima column 5 lines 19-20); and if not, then broadcasting an ARP request with the destination IP address and receiving an ARP reply with the MAC address (see Kojima column 5 lines 17-35). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have added a MAC address to the data get to help the data get delivered to its destination across the LAN (see Kojima column 5 lines 17-35). Therefore one would have been motivated to have add a MAC address.

With respect to claim 6, wherein the IP-encapsulated encrypted packet is communicated across multiple intermediate layer 2 domains (see Amara figure 1).

Claim 12, rejected under 35 U.S.C. 103(a) as being unpatentable over Regan (U.S. 2004/0213232) in view of Amara et al (U.S. Patent # 6,839,338) in view of Classon et al (U.S. Patent 6,700,867). Regan and Amara teaches everything with respect to claim 1 above but does not teach truncating the data packet to reduce a size of the data packet prior to encryption. Classon teaches truncating the data packet to reduce a size of the data packet prior to encryption (see column 20 lines 20-53). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have truncated the data packet to satify memory (buffer) requirements (see column 20 lines 20-53). Therefore one would have been motivated to have truncated the data packet.

Claim 13, rejected under 35 U.S.C. 103(a) as being unpatentable over Regan (U.S. 2004/0213232) in view of Amara et al (U.S. Patent # 6,839,338) in view of Engwer (U.S. Patent 6,947,483). Regan and Amara teaches everything with respect to claim 1 above but does not teach compressing at least a portion of the data packet to reduce a size of the data packet prior to encryption. Engwer teaches compressing at least a portion of the data packet to reduce a size of the data packet prior to encryption (see column 1 line 52 – column 2 line 6). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have compressed the data packet. Data transmission between the various access points (APs) and their associated mobile units may involve large

amounts of data which may take substantial amount of time and processing power to transmit over the air median. Such data transmissions are costly if the transmitted data is uncompressed.s (see column 1 line 52 – column 2 line 6). Therefore one would have been motivated to have compressed the data packet.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Devin Almeida/
Examiner, Art Unit 2132
10/01/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132